A complete characterization of irreducible cyclic orbit codes and their Plücker embedding

Rosenthal, J ; Trautmann, A L

Abstract: Constant dimension codes are subsets of the finite Grassmann variety. The study of these codes is a central topic in random linear network coding theory. Orbit codes represent a subclass of constant dimension codes. They are defined as orbits of a subgroup of the general linear group on the Grassmannian. This paper gives a complete characterization of orbit codes that are generated by an irreducible cyclic group, i.e. a group having one generator that has no non-trivial invariant subspace. We show how some of the basic properties of these codes, the cardinality and the minimum distance, can be derived using the isomorphism of the vector space and the extension field. Furthermore, we investigate the Plücker embedding of these codes and show how the orbit structure is preserved in the embedding.

DOI: https://doi.org/10.1007/s10623-012-9691-5

Des. Codes Cryptogr. (2013) 66:275–289
DOI 10.1007/s10623-012-9691-5

A complete characterization of irreducible cyclic orbit codes and their Plücker embedding

Joachim Rosenthal · Anna-Lena Trautmann

Received: 5 September 2011 / Revised: 29 February 2012 / Accepted: 30 April 2012 /
Published online: 19 May 2012

Abstract Constant dimension codes are subsets of the finite Grassmann variety. The study of these codes is a central topic in random linear network coding theory. Orbit codes represent a subclass of constant dimension codes. They are defined as orbits of a subgroup of the general linear group on the Grassmannian. This paper gives a complete characterization of orbit codes that are generated by an irreducible cyclic group, i.e. a group having one generator that has no non-trivial invariant subspace. We show how some of the basic properties of these codes, the cardinality and the minimum distance, can be derived using the isomorphism of the vector space and the extension field. Furthermore, we investigate the Plücker embedding of these codes and show how the orbit structure is preserved in the embedding.

Keywords Network coding · Constant dimension codes · Grassmannian · Plücker embedding · Projective space · General linear group

Mathematics Subject Classification 11T71

1 Introduction

In network coding one is looking at the transmission of information through a directed graph with possibly several senders and several receivers [1]. One can increase the throughput by linearly combining the information vectors at intermediate nodes of the network. If the underlying topology of the network is unknown we speak about *random linear network coding*. Since linear spaces are invariant under linear combinations, they are what is needed as

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Coding and Cryptography".

J. Rosenthal · A.-L. Trautmann (✉)
Institute of Mathematics, University of Zurich, Zurich, Switzerland
e-mail: anna-lena.trautmann@math.uzh.ch
URL: www.math.uzh.ch/aa

codewords [7]. It is helpful (e.g. for decoding) to constrain oneself to subspaces of a fixed dimension, in which case we talk about *constant dimension codes*.

The set of all k-dimensional subspaces of a vector space V is often referred to as the Grassmann variety (or simply Grassmannian) and denoted by $\mathcal{G}(k, V)$. *Constant dimension codes* are subsets of $\mathcal{G}(k, \mathbb{F}_q^n)$, where $\mathbb{F}_q$ is some finite field.

The general linear group $\mathrm{GL}(V)$ consisting of all invertible transformations acts naturally on the Grassmannian $\mathcal{G}(k, V)$. If $\mathfrak{G} \leq \mathrm{GL}(\mathbb{F}_q^n)$ is a subgroup then one has an induced action of $\mathfrak{G}$ on the finite Grassmannian $\mathcal{G}(k, \mathbb{F}_q^n)$. Orbits under the $\mathfrak{G}$-action are called *orbit codes* [13]. Orbit codes have useful algebraic structure, e.g. for the computation of the distance of an orbit code it is enough to compute the distance between the starting point and any of its orbit elements. This is analogous to linear block codes where the minimum distance of the code can be derived from the weights of the non-zero code words.

Orbit codes can be classified according to the groups used to construct the orbit. In this work we characterize orbit codes generated by irreducible cyclic subgroups of the general linear group and their Plücker embedding.

The paper is structured as follows: The second section gives some preliminaries, first of random network coding and orbit codes. Then some facts on irreducible polynomials are stated and the representation of finite vector spaces as Galois extension fields is explained in 2.2. In part 2.3 we introduce irreducible matrix groups and give some properties, with a focus on the cyclic ones. The main body of the paper are Sects. 3 and 4. In the former we study the behavior of orbit codes generated by these groups and compute the cardinality and minimum distances of them. We begin by characterizing primitive orbit codes and then study the non-primitive irreducible ones. Section 4 deals with the Plücker embedding of cyclic irreducible orbit codes. Finally we give a conclusion and an outlook in Sect. 5.

2 Preliminaries

2.1 Random network codes

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. For simplicity we will denote the Grassmannian $\mathcal{G}(k, \mathbb{F}_q^n)$ by $\mathcal{G}_q(k, n)$ and the general linear group, that is the set of all invertible $n \times n$-matrices with entries in $\mathbb{F}_q$, by GL_n. Moreover, the set of all $k \times n$-matrices over $\mathbb{F}_q$ is denoted by $\mathrm{Mat}_{k\times n}$.

Let $U \in \mathrm{Mat}_{k\times n}$ be a matrix of rank k and

$$\mathcal{U} = \mathrm{rs}(U) := \text{row space}(U) \in \mathcal{G}_q(k, n).$$

One can notice that the row space is invariant under GL_k-multiplication from the left, i.e. for any $T \in \mathrm{GL}_k$

$$\mathcal{U} = \mathrm{rs}(U) = \mathrm{rs}(TU).$$

Thus, there are several matrices that represent a given subspace. A unique representative of these matrices is the one in reduced row echelon form. Any $k \times n$-matrix can be transformed into reduced row echelon form by a $T \in \mathrm{GL}_k$.

The set of all subspaces of $\mathbb{F}_q^n$, called the projective geometry of $\mathbb{F}_q^n$, is denoted by $\mathrm{PG}(\mathbb{F}_q^n)$. The *subspace distance* is a metric on it, given by

$$d_S(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U} \cap \mathcal{V})$$

for any $\mathcal{U}, \mathcal{V} \in \mathrm{PG}(\mathbb{F}_q^n)$. It is a suitable distance for coding over the operator channel [7].

A *constant dimension code* $\mathcal{C}$ is simply a subset of the Grassmannian $\mathcal{G}_q(k,n)$. The minimum distance is defined in the usual way. A code $\mathcal{C} \subset \mathcal{G}_q(k,n)$ with minimum distance $d_S(\mathcal{C})$ is called an $[n, d_S(\mathcal{C}), |\mathcal{C}|, k]$-code. Different constructions of constant dimension codes can be found in e.g. [3,6,7,9,12,13].

In the case that k divides n one can construct *spread codes* [9], i.e. optimal codes with minimum distance $2k$. These codes are optimal because they achieve the Singleton-like bound [7], which means they have $\frac{q^n-1}{q^k-1}$ elements.

Given $U \in \mathrm{Mat}_{k\times n}$ of rank k, $\mathcal{U} \in \mathcal{G}_q(k,n)$ its row space and $A \in \mathrm{GL}_n$, we define

$$\mathcal{U}A := \mathrm{rs}(UA).$$

Let $U, V \in \mathrm{Mat}_{k\times n}$ be matrices such that $\mathrm{rs}(U) = \mathrm{rs}(V)$. Then one readily verifies that $\mathrm{rs}(UA) = \mathrm{rs}(VA)$ for any $A \in \mathrm{GL}_n$. The subspace distance is GL_n-invariant, i.e. $d_S(\mathcal{U},\mathcal{V}) = d_S(\mathcal{U}A, \mathcal{V}A)$ for $A \in \mathrm{GL}_n$.

This multiplication with GL_n-matrices defines a group operation from the right on the Grassmannian:

$$\begin{array}{ccc} \mathcal{G}_q(k,n) \times \mathrm{GL}_n & \longrightarrow & \mathcal{G}_q(k,n) \\ (\mathcal{U}, A) & \longmapsto & \mathcal{U}A \end{array}$$

Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ be fixed and $\mathfrak{G}$ a subgroup of GL_n. Then

$$\mathcal{C} = \{\mathcal{U}A \mid A \in \mathfrak{G}\}$$

is called an *orbit code* [13]. It is well-known that

$$\mathcal{G}_q(k,n) \cong \mathrm{GL}_n / Stab_{\mathrm{GL}_n}(\mathcal{U}),$$

where $Stab_{\mathrm{GL}_n}(\mathcal{U}) := \{A \in \mathrm{GL}_n \mid \mathcal{U}A = \mathcal{U}\}$. There are different subgroups that generate the same orbit code. An orbit code is called *cyclic* if it can be defined by a cyclic subgroup $\mathfrak{G} \leq \mathrm{GL}_n$.

2.2 Irreducible polynomials and extension fields

Let us state some known facts on irreducible polynomials over finite fields [8, Lemmas 3.4 – 3.6]:

Lemma 1 *Let $p(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n, $p(0) \neq 0$ and α a root of it. Define the order of $p(x)$ as the smallest integer e for which $p(x)$ divides $x^e - 1$. Then*

1. *the order of $p(x)$ is equal to the order of α in $\mathbb{F}_{q^n}\backslash\{0\}$.*
2. *the order of $p(x)$ divides $q^n - 1$.*
3. *$p(x)$ divides $x^c - 1$ if, and only if the order of $p(x)$ divides c (where $c \in \mathbb{N}$).*

There is an isomorphism between the vector space $\mathbb{F}_q^n$ and the Galois extension field $\mathbb{F}_{q^n} \cong \mathbb{F}_q[\alpha]$, for α a root of an irreducible polynomial $p(x)$ of degree n over $\mathbb{F}_q$. If in addition $p(x)$ is primitive, then

$$\mathbb{F}_q[\alpha]\backslash\{0\} = \langle\alpha\rangle = \{\alpha^i \mid i = 0, \ldots, q^n - 2\}$$

i.e. α generates multiplicatively the group of invertible elements of the extension field.

Lemma 2 *If $k|n$, $c := \frac{q^n-1}{q^k-1}$ and α is a primitive element of $\mathbb{F}_{q^n}$, then the vector space generated by $1, \alpha^c, \ldots, \alpha^{(k-1)c}$ is equal to $\{\alpha^{ic} \mid i = 0, \ldots, q^k - 2\} \cup \{0\} = \mathbb{F}_{q^k}$.*

Proof Since $k|n$ it holds that $c \in \mathbb{N}$. Moreover, it holds that $(\alpha^c)^{q^k-1} = \alpha^{q^n-1} = 1$ and $(\alpha^c)^{q^k-2} = \alpha^{-c} \neq 1$, hence the order of α^c is $q^k - 1$. It is well-known that if k divides n the field $\mathbb{F}_{q^n}$ has exactly one subfield $\mathbb{F}_{q^k}$. Thus the group generated by α^c has to be $\mathbb{F}_{q^k}\backslash\{0\}$, which again is isomorphic to $\mathbb{F}_q^k$ as a vector space. □

2.3 Irreducible matrix groups

Definition 3 1. A matrix $A \in \mathrm{GL}_n$ is called *irreducible* if $\mathbb{F}_q^n$ contains no non-trivial A-invariant subspace, otherwise it is called *reducible*.
2. A subgroup $\mathfrak{G} \leq \mathrm{GL}_n$ is called *irreducible* if $\mathbb{F}_q^n$ contains no non-trivial $\mathfrak{G}$-invariant subspace, otherwise it is called *reducible*.
3. An orbit code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ is called *irreducible* if $\mathcal{C}$ is the orbit under the action of an irreducible group.

A cyclic group is irreducible if and only if its generator matrix is irreducible. Moreover, an invertible matrix is irreducible if and only if its characteristic polynomial is irreducible.

Example 4 Over $\mathbb{F}_2$ the only irreducible polynomial of degree 2 is $p(x) = x^2 + x + 1$. Since their characteristic polynomial has to be $p(x)$, the irreducible matrices in GL_2 must have trace and determinant equal to 1 and hence are

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

We can say even more about irreducible matrices with the same characteristic polynomial. For this, note that the definition of an irreducible matrix G implies the existence of a *cyclic vector* $v \in \mathbb{F}_q^n$ having the property that

$$\left\{v, vG, vG^2, \ldots, vG^{n-1}\right\}$$

forms a basis of $\mathbb{F}_q^n$. Let $S \in \mathrm{GL}_n$ be the basis transformation which transforms the matrix G into this new basis. Then it follows that

$$SGS^{-1} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ -c_0 & -c_1 & & \ldots & -c_{n-1} \end{pmatrix}.$$

The matrix appearing on the right is said to be in *companion form*. By convention we will use row vectors $v \in \mathbb{F}_q^n$ and accordingly companion matrices where the coefficients of the corresponding polynomials are in the last row (instead of the last column).

One readily verifies that

$$p(x) := x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

is the characteristic polynomial of both G and SGS^{-1}. It follows that every irreducible matrix in GL_n is similar to the companion matrix of its characteristic polynomial. Hence all irreducible matrices with the same characteristic polynomial are similar.

Furthermore, the order of $G \in \mathrm{GL}_n$ is equal to the order of its characteristic polynomial. Hence $\mathrm{ord}(G) = q^n - 1$ if and only if its characteristic polynomial is primitive.

The next fact is a well-known group theoretic result:

Lemma 5 [8, Theorem 1.15.] *In a finite cyclic group $\mathfrak{G} = \langle G \rangle$ of order m, the element G^l generates a subgroup of order $\frac{m}{\gcd(l,m)}$. Hence each element G^l with $\gcd(l, m) = 1$ is a generator of $\mathfrak{G}$.*

Lemma 6 [10, Theorem 7] *All irreducible cyclic groups generated by matrices with a characteristic polynomial of the same order are conjugate to each other.*

Example 7 Over $\mathbb{F}_2$ the irreducible polynomials of degree 4 are $p_1(x) = x^4+x+1$, $p_2(x) = x^4 + x^3 + 1$ and $p_3(x) = x^4 + x^3 + x^2 + x + 1$, where $\mathrm{ord}(p_1) = \mathrm{ord}(p_2) = 15$ and $\mathrm{ord}(p_3) = 5$. Let P_1, P_2, P_3 be the respective companion matrices. One verifies that $\langle P_1 \rangle$ and $\langle P_2 \rangle$ are conjugate to each other but $\langle P_3 \rangle$ is not conjugate to them.

One can describe the action of an irreducible matrix group via the Galois extension field isomorphism.

Theorem 8 *Let $p(x)$ be a monic irreducible polynomial over $\mathbb{F}_q$ of degree n and P its companion matrix. Furthermore let $\alpha \in \mathbb{F}_{q^n}$ be a root of $p(x)$ and ϕ be the canonical homomorphism*

$$\begin{aligned} \phi : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_{q^n} \cong \mathbb{F}_q[\alpha] \\ (v_1, \ldots, v_n) &\longmapsto \sum_{i=1}^{n} v_i \alpha^{i-1}. \end{aligned}$$

Then the following diagram commutes (for $v \in \mathbb{F}_q^n$):

$$\begin{array}{ccc} v & \xrightarrow{\cdot P} & vP \\ \phi \downarrow & & \downarrow \phi \\ v' & \xrightarrow[\cdot \alpha]{} & v'\alpha \end{array}$$

If P is a companion matrix of a primitive polynomial the group generated by P is also known as a *Singer group*. This notation is used e.g. by Kohnert et al. in their network code construction [2,6]. Elsewhere P is called *Singer cycle* or *cyclic projectivity* (e.g. in [4]).

3 Irreducible cyclic orbit codes

The irreducible cyclic subgroups of GL_n are exactly the groups generated by the companion matrices of the irreducible polynomials of degree n and their conjugates. Moreover, all groups generated by companion matrices of irreducible polynomials of the same order are conjugate.

The following theorem shows that it is sufficient to characterize the orbits of cyclic groups generated by companion matrices of irreducible polynomials of degree n.

Theorem 9 *Let G be an irreducible matrix, $\mathfrak{G} = \langle G \rangle$ and $\mathfrak{H} = \langle S^{-1}GS \rangle$ for an $S \in \mathrm{GL}_n$. Moreover, let $\mathcal{U} \in \mathcal{G}_q(k, n)$ and $\mathcal{V} := \mathcal{U}S$. Then the orbit codes*

$$\mathcal{C} := \{\mathcal{U}A \mid A \in \mathfrak{G}\} \text{ and } \mathcal{C}' := \{\mathcal{V}B \mid B \in \mathfrak{H}\}$$

have the same cardinality and minimum distance.

Proof Trivially the cardinality of both codes is the same. It remains to be shown that the same holds for the minimum distance.

Since

$$\mathcal{V}(S^{-1}GS)^i = \mathcal{V}S^{-1}G^iS = \mathcal{U}SS^{-1}G^iS = \mathcal{U}G^iS$$

and the subspace distance is invariant under GL_n-action, it holds that

$$d_S(\mathcal{U}, \mathcal{U}G^i) = d_S(\mathcal{V}, \mathcal{U}G^iS)$$

hence the minimum distances of the codes defined by $\mathfrak{G}$ and by $\mathfrak{H}$ are equal. □

3.1 Primitive generator

Let α be a primitive element of $\mathbb{F}_{q^n}$ and assume $k|n$ and $c := \frac{q^n-1}{q^k-1}$. Naturally, the subfield $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$ is also an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$. On the other hand, $\mathbb{F}_{q^k} = \{\alpha^{ic} \mid i = 0, \ldots, q^k - 2\} \cup \{0\}$.

Lemma 10 *For every $\beta \in \mathbb{F}_{q^n}$ the set*

$$\beta \cdot \mathbb{F}_{q^k} = \left\{\beta\alpha^{ic} \mid i = 0, \ldots, q^k - 2\right\} \cup \{0\}$$

defines an $\mathbb{F}_q$-subspace of dimension k.

Proof Since $\mathbb{F}_{q^k}$ is a subspace of dimension k and

$$\begin{aligned} \varphi_\beta : \mathbb{F}_{q^n} &\longrightarrow \mathbb{F}_{q^n} \\ u &\longmapsto \beta u \end{aligned}$$

is an $\mathbb{F}_q$-linear isomorphism, it follows that $\varphi_\beta(\mathbb{F}_{q^k}) = \beta \cdot \mathbb{F}_{q^k}$ is an $\mathbb{F}_q$-subspace of dimension k. □

Theorem 11 *The set*

$$\mathcal{S} = \left\{\alpha^i \cdot \mathbb{F}_{q^k} \mid i = 0, \ldots, c - 1\right\}$$

is a spread of $\mathbb{F}_{q^n}$ and thus defines a spread code in $\mathcal{G}_q(k, n)$.

Proof By a simple counting argument it is enough to show that the subspace $\alpha^i \cdot \mathbb{F}_{q^k}$ and $\alpha^j \cdot \mathbb{F}_{q^k}$ have only trivial intersection whenever $0 \leq i < j \leq c - 1$. For this assume that there are field elements $c_i, c_j \in \mathbb{F}_{q^k}$, such that

$$v = \alpha^i c_i = \alpha^j c_j \in \alpha^i \cdot \mathbb{F}_{q^k} \cap \alpha^j \cdot \mathbb{F}_{q^k}.$$

If $v \neq 0$ then $\alpha^{i-j} = c_j c_i^{-1} \in \mathbb{F}_{q^k}$. But this means $i - j \equiv 0 \mod c$ and $\alpha^i \cdot \mathbb{F}_{q^k} = \alpha^j \cdot \mathbb{F}_{q^k}$, which contradicts the assumption. It follows that $\mathcal{S}$ is a spread. □

We now translate this result into a matrix setting. For this let ϕ denote the canonical homomorphism as defined in Theorem 8.

Corollary 12 *Assume $k|n$. Then there is a subspace $\mathcal{U} \in \mathcal{G}_q(k, n)$ such that the cyclic orbit code obtained by the group action of a a primitive companion matrix is a code with minimum distance $2k$ and cardinality $\frac{q^n-1}{q^k-1}$. Hence this irreducible cyclic orbit code is a spread code.*

Proof In the previous theorem represent $\mathbb{F}_{q^k} \subset \mathbb{F}_{q^n}$ as the row space of a $k \times n$ matrix U over $\mathbb{F}_q$ and, using the same basis over $\mathbb{F}_q$, represent the primitive element α with its respective companion matrix P. Then the orbit code $\mathcal{C} = \mathrm{rs}(U)\langle P\rangle$ has all the desired properties. □

Example 13 Consider the binary field and let $p(x) := x^6 + x + 1$, which is a primitive polynomial of degree 6. Let α be a root of $p(x)$ and P its companion matrix.

1. For the 3-dimensional spread compute $c = \frac{63}{7} = 9$ and construct a basis for the starting point of the orbit:

$$u_1 = \phi^{-1}(\alpha^0) = \phi^{-1}(1) = (100000)$$
$$u_2 = \phi^{-1}(\alpha^c) = \phi^{-1}(\alpha^9) = \phi^{-1}(\alpha^4 + \alpha^3) = (000110)$$
$$u_3 = \phi^{-1}(\alpha^{2c}) = \phi^{-1}(\alpha^{18}) = \phi^{-1}(\alpha^3 + \alpha^2 + \alpha + 1) = (111100)$$

   The starting point is

$$\mathcal{U} = \mathrm{rs}\begin{bmatrix} 1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,1\,0 \\ 1\,1\,1\,1\,0\,0 \end{bmatrix} = \mathrm{rs}\begin{bmatrix} 1\,0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,1\,0 \\ 0\,0\,0\,1\,1\,0 \end{bmatrix}$$

   and the orbit of the group generated by P on $\mathcal{U}$ is a spread code.
2. For the 2-dimensional spread compute $c = \frac{63}{3} = 21$ and construct the starting point

$$u_1 = \phi^{-1}(\alpha^0) = \phi^{-1}(1) = (100000)$$
$$u_2 = \phi^{-1}(\alpha^c) = \phi^{-1}(\alpha^{21}) = \phi^{-1}(\alpha^2 + \alpha + 1) = (111000)$$

   The starting point is

$$\mathcal{U} = \mathrm{rs}\begin{bmatrix} 1\,0\,0\,0\,0\,0 \\ 1\,1\,1\,0\,0\,0 \end{bmatrix} = \mathrm{rs}\begin{bmatrix} 1\,0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,0\,0 \end{bmatrix}$$

   and the orbit of the group generated by P is a spread code.

Remark 14 Spreads are well-known geometrical objects and have been studied from a coding perspective in e.g. [9,11]. They are the only known optimal constant dimension codes, i.e. their cardinality $\frac{q^n-1}{q^k-1}$ reaches the Singleton-like bound on the size of constant dimension codes. They always have minimum distance $2k$ and rate

$$\frac{\log_q\left(\frac{q^n-1}{q^k-1}\right)}{nk} \approx \frac{n-k}{nk} \xrightarrow{n\to\infty} \frac{1}{k}.$$

For more information on the Singleton-like bound and rates of random network codes the reader is referred to [7].

The following fact is a generalization of Lemma 1 from [6].

Theorem 15 *Assume* $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k, n)$,

$$\phi(u_i) = \alpha^{b_i} \qquad \forall i = 1, \ldots, q^k - 1$$

and $d \in \mathbb{N}$ *be minimal such that any element of the set*

$$D := \left\{ b_m - b_l \mod q^n - 1 \mid l, m \in \mathbb{Z}_{q^k-1}, l \neq m \right\}$$

has multiplicity less than or equal to $q^d - 1$, i.e. a quotient of two elements in the field representation appears at most $q^d - 1$ times in the set of all pairwise quotients. If $d < k$ then the orbit of the group generated by the companion matrix P of $p(x)$ on $\mathcal{U}$ is an orbit code of cardinality $q^n - 1$ and minimum distance $2k - 2d$.

Proof In field representation the elements of the orbit code are:

$$\begin{aligned} C_0 &= \left\{\alpha^{b_1}, \alpha^{b_2}, \ldots, \alpha^{b_{q^k-1}}\right\} \cup \{0\} \\ C_1 &= \left\{\alpha^{b_1+1}, \alpha^{b_2+1}, \ldots, \alpha^{b_{q^k-1}+1}\right\} \cup \{0\} \\ &\vdots \\ C_{q^n-2} &= \left\{\alpha^{b_1+q^n-2}, \ldots, \alpha^{b_{q^k-1}+q^n-2}\right\} \cup \{0\} \end{aligned}$$

Assume without loss of generality that the first $q^d - 1$ elements of C_h are equal to the last elements of C_j:

$$\begin{aligned} \alpha^{b_1+h} = \alpha^{b_{q^k-q^{d+1}}+j} &\iff b_1 + h \equiv b_{q^k-q^{d+1}} + j \mod q^n - 1 \\ &\vdots \\ \alpha^{b_{q^{d-1}}+h} = \alpha^{b_{q^k-1}+j} &\iff b_{q^{d-1}} + h \equiv b_{q^k-1} + j \mod q^n - 1 \end{aligned}$$

To have another element in common there have to exist y and z such that

$$b_{q^k-q^{d+1}} - b_1 \equiv b_z - b_y \mod q^n - 1.$$

But by condition there are up to $q^d - 1$ solutions in (y, z) for this equation, including the ones from above. Thus the intersection of C_i and C_j has at most $q^d - 1$ non-zero elements. On the other hand, one can always find $h \neq j$ such that there are $q^d - 1$ solutions to

$$b_y + h \equiv b_z + j \mod q^n - 1,$$

hence, the minimum distance is exactly $2k - 2d$. □

Proposition 16 *In the setting of before, if $d = k$, one gets orbit elements with full intersection which means they are the same vector space.*

1. *Let $m(a)$ denote the multiplicity of an element in the respective set and $D' := D \backslash \{a \in D \mid m(a) = q^k - 1\}$. Then the minimum distance of the code is $2k - 2d'$ where $d' := \log_q(\max\{m(a) \mid a \in D'\})$.*
2. *Let m be the least element of D of multiplicity $q^k - 1$. Then the cardinality of the code is $m - 1$.*

Proof 1. Since the minimum distance of the code is only taken between distinct vector spaces, one has to consider the largest intersection of two elements whose dimension is less than k.

2. Since

$$\mathcal{U}P^m = \mathcal{U} \implies \mathcal{U}P^{lm} = \mathcal{U} \quad \forall l \in \mathbb{N}$$

and the elements of D are taken modulo the order of P, one has to choose the minimal element of the set $\{a \in D \mid m(a) = q^k - 1\}$ for the number of distinct vector spaces in the orbit. □

3.2 Non-primitive generator

Theorem 17 *Let P be an irreducible non-primitive companion matrix, $\mathfrak{G}$ the group generated by it and denote by $v\mathfrak{G}$ and $\mathcal{U}\mathfrak{G}$ the orbits of $\mathfrak{G}$ on $v \in \mathbb{F}_q^n$ and $\mathcal{U} \in \mathcal{G}_q(k,n)$, respectively. If $\mathcal{U} \in \mathcal{G}_q(k,n)$ such that*

$$v \neq w \implies v\mathfrak{G} \neq w\mathfrak{G} \quad \forall\, v, w \in \mathcal{U},$$

then $\mathcal{U}\mathfrak{G}$ is an orbit code with minimum distance $2k$ and cardinality $\mathrm{ord}(P)$.

Proof The cardinality follows from the fact that each element of $\mathcal{U}$ has its own orbit of length $\mathrm{ord}(P)$. Moreover, no code words intersect non-trivially, hence the minimum distance is $2k$. □

Note that, if the order of P is equal to $\frac{q^n-1}{q^k-1}$, these codes are again spread codes.

Example 18 Over the binary field let $p(x) = x^4 + x^3 + x^2 + x + 1$, α a root of $p(x)$ and P its companion matrix. Then $\mathbb{F}_{2^4}\backslash\{0\}$ is partitioned into

$$\left\{\alpha^i \mid i = 0, \ldots, 4\right\} \cup \left\{\alpha^i\,(\alpha+1) \mid i = 0, \ldots, 4\right\} \cup \left\{\alpha^i\left(\alpha^2+1\right) \mid i = 0, \ldots, 4\right\}.$$

Choose

$$\begin{aligned} u_1 &= \phi^{-1}(1) = \phi^{-1}\left(\alpha^0\right) = (1000) \\ u_2 &= \phi^{-1}\left(\alpha^3+\alpha^2\right) = \phi^{-1}\left(\alpha^2(\alpha+1)\right) = (0011) \\ u_3 &= u_1 + u_2 = \phi^{-1}\left(\alpha^3+\alpha^2+1\right) = \phi^{-1}\left(\alpha^4\left(\alpha^2+1\right)\right) = (1011) \end{aligned}$$

such that each u_i is in a different orbit of $\langle P\rangle$ and $\mathcal{U} = \{0, u_1, u_2, u_3\}$ is a vector space. Then the orbit of $\langle P\rangle$ on $\mathcal{U}$ has minimum distance 4 and cardinality 5, hence it is a spread code.

Proposition 19 *Let P and $\mathfrak{G}$ be as before and $\mathcal{U} = \{0, v_1, \ldots, v_{q^k-1}\} \in \mathcal{G}_q(k,n)$. Let $l = \frac{q^n-1}{ord(P)}$ and $O_1, \ldots, O_l$ be the different orbits of $\mathfrak{G}$ in $\mathbb{F}_q^n$. Assume that $m < q^k - 1$ elements of $\mathcal{U}$ are in the same orbit, say O_1, and all other elements are in different orbits each, i.e.*

$$v_i\mathfrak{G} = v_j\mathfrak{G} = O_1 \quad \forall\, i, j \leq m,$$

$$v_i \neq v_j \implies v_i\mathfrak{G} \neq v_j\mathfrak{G} \quad \forall\, i, j \geq m.$$

Apply the theory of Sect. 3.1 to the orbit O_1 and find d_1 fulfilling the conditions of Theorem 15. Then the orbit of $\mathfrak{G}$ on $\mathcal{U}$ is a code of length $\mathrm{ord}(P)$ *and minimum distance $2k - 2d_1$.*

Proof 1. Since there is at least one orbit O_i that contains exactly one element of $\mathcal{U}$, each element of O_i is in exactly one code word. Hence the cardinality of the code is $\mathrm{ord}(\mathfrak{G}) = \mathrm{ord}(P)$.

2. In analogy to Theorem 17 the only possible intersection is inside O_1, which can be found according to the theory of primitive cyclic orbit codes. □

We generalize these results to any possible starting point $\in \mathcal{G}_q(k,n)$:

Theorem 20 *Let $P, \mathfrak{G}, \mathcal{U}$ and the orbits $O_1, \ldots, O_l$ be as before. Assume that m_i elements of $\mathcal{U}$ are in the same orbit O_i $(i = 1, \ldots, l)$. Apply the theory of Sect. 3.1 to each orbit O_i and find the corresponding d_i from Theorem 15. Then the following cases can occur:*

1. *No intersections of two different orbits coincide. Define* $d_{\max} := \max_i d_i$. *Then the orbit of* $\mathfrak{G}$ *on* $\mathcal{U}$ *is a code of length* $\mathrm{ord}(P)$ *and minimum distance* $2k - 2d_{max}$.
2. *Some intersections coincide among some orbits. Then the corresponding* d_i*'s add up and the maximum of these is the maximal intersection number* $d_{\max}$.

Mathematically formulated: Assume $b_{(i,1)}, \ldots, b_{(i,\mathrm{ord}(P)-1)}$ *are the exponents of the field representation of the non-zero elements of* $\mathcal{U}$ *on* O_i. *For* $i = 1, \ldots, l$ *define*

$$a_{(i,\mu,\lambda)} := b_{(i,\mu)} - b_{(i,\lambda)},$$

$$D_i := \left\{ a_{(i,\mu,\lambda)} \mid \mu, \lambda \in \{1, \ldots, \mathrm{ord}(P) - 1\} \right\},$$

and the difference set

$$D := \bigcup_{i=1}^{l} D_i .$$

Denote by $m(a)$ *the multiplicity of an element* a *in* D *and* $d_{\max} := \log_q(\max\{m(a) \mid a \in D\}+1)$. *Then the orbit of* $\mathfrak{G}$ *on* $\mathcal{U}$ *is a code of length* $\mathrm{ord}(P)$ *and minimum distance* $2k-2d_{\max}$.

Again note that, in the case that the minimum distance of the code is 0, one has double elements in the orbit. Then Proposition 16 still holds.

Remark 21 The theorems about the minimum distance can also be used for the construction of orbit codes with a prescribed minimum distance. For this construct the initial point of the orbit by iteratively joining elements $\alpha^i \in \mathbb{F}_{q^k}$ such that the linear span of the union fulfills the condition on the differences of the exponents.

4 Plücker embedding

For the remainder of this paper let $p(x) = \sum_{i=0}^{n} p_i x^i \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n and α a root of it. The companion matrix of $p(x)$ is denoted by P. $\mathbb{F}_q^{\times} := \mathbb{F}_q \backslash \{0\}$ is the set of all invertible elements of $\mathbb{F}_q$.

Moreover, let $A \in \mathrm{Mat}_{m\times n}$ such that $m, n \geq k$. Denote by $A_{i_1,\ldots,i_k}[j_1, \ldots, j_k]$ the $k \times k$ submatrix of A defined by rows $i_1, \ldots, i_k$ and columns $j_1, \ldots, j_k$ and $A[j_1, \ldots, j_k]$ denotes the submatrix of A with the complete columns $j_1, \ldots, j_k$.

Definition 22 We define the following operation on $\Lambda^k(\mathbb{F}_q[\alpha]) \cong \Lambda^k(\mathbb{F}_q^n)$:

$$\begin{aligned} * : \Lambda^k\left(\mathbb{F}_q[\alpha]\right) \times \mathbb{F}_q[\alpha]\backslash\{0\} &\longrightarrow \Lambda^k\left(\mathbb{F}_q[\alpha]\right) \\ \left((v_1 \wedge \ldots \wedge v_2), \beta\right) &\longmapsto (v_1 \wedge \ldots \wedge v_2) * \beta := (v_1\beta \wedge \ldots \wedge v_k\beta) . \end{aligned}$$

This is a group action since $((v_1 \wedge \ldots \wedge v_2) * \beta) * \gamma = (v_1 \wedge \ldots \wedge v_2) * (\beta\gamma)$.

Theorem 23 *The following maps are (isomorphic) embeddings of the Grassmannian:*

$$\begin{aligned} \varphi : \mathcal{G}_q(k,n) &\longrightarrow \mathbb{P}^{\binom{n}{k}-1} \\ \mathrm{rs}(U) &\longmapsto [\det(U[1,\ldots,k]) : \det(U[1,\ldots,k-1,k+1]) : \ldots : \\ &\qquad \det(U[n-k+1,\ldots,n])] \\ \varphi' : \mathcal{G}_q(k,n) &\longrightarrow \mathbb{P}(\Lambda^k(\mathbb{F}_q[\alpha])) \\ \mathrm{rs}(U) &\longmapsto (\phi(U_1) \wedge \ldots \wedge \phi(U_k)) * \mathbb{F}_q^{\times} \end{aligned}$$

where $\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ *denotes the standard vector space isomorphism.*

Proof First we show that φ is an embedding. For this assume that U, V are two full-rank $k \times n$ matrices such that $\mathrm{rs}(U) = \mathrm{rs}(V)$. It follows that there is an $S \in \mathrm{GL}_k$ with $V = SU$. The two vectors

$$[\det(U[1,\ldots,k]), \det(U[1,\ldots,k-1,k+1]), \ldots, \det(U[n-k+1,\ldots,n])]$$

and

$$[\det(V[1,\ldots,k]), \det(V[1,\ldots,k-1,k+1]), \ldots, \det(V[n-k+1,\ldots,n])]$$

differ hence only by the non-zero factor $\det S$. As elements of the projective space $\mathbb{P}^{\binom{n}{k}-1}$ they are thus the same and the map is well defined.

Assume now that $\mathrm{rs}(U) \neq \mathrm{rs}(V)$. Without loss of generality we can assume that both U and V are in reduced row echelon form, where the forms are necessarily different. Observe that all non-zero entries of U can also be written, up to sign, as $\det(U[i_1,\ldots,i_k])$. It follows that $\varphi(U)$ is different from $\varphi(V)$.

Next we show that the map $\psi : \varphi'(\mathcal{G}_q(k,n)) \to \varphi(\mathcal{G}_q(k,n))$, defined as follows, is an isomorphism.

$$\begin{aligned}
(\phi(U_1) \wedge \cdots \wedge \phi(U_k)) * \mathbb{F}_q^\times &= \left(\sum_{i=0}^{n-1} \lambda_{1i}\alpha^i \wedge \cdots \wedge \sum_{i=0}^{n-1} \lambda_{ki}\alpha^i\right) * \mathbb{F}_q^\times \\
&= \sum_{0\le i_1,\ldots,i_k<n} \left(\lambda_{1i_1}\alpha^{i_1} \wedge \cdots \wedge \lambda_{ki_k}\alpha^{i_k}\right) * \mathbb{F}_q^\times \\
&= \sum_{0\le i_1,\ldots,i_k<n} \lambda_{1i_1}\ldots\lambda_{ki_k}\left(\alpha^{i_1} \wedge \cdots \wedge \alpha^{i_k}\right) * \mathbb{F}_q^\times \\
&= \sum_{0\le i_1<\ldots<i_k<n} \mu_{i_1,\ldots,i_k}\left(\alpha^{i_1} \wedge \cdots \wedge \alpha^{i_k}\right) * \mathbb{F}_q^\times \\
&\longmapsto \left[\mu_{0,\ldots,k-1} : \ldots : \mu_{n-k,\ldots,n-1}\right]
\end{aligned}$$

where $\lambda_{jl} \in \mathbb{F}_q$ for all $j \in \{1,\ldots,k\}, l \in \{0,\ldots,n-1\}$ and $\mu_{i_1,\ldots,i_k} := \sum_{\sigma\in S_k}(-1)^\sigma \lambda_{1\sigma(i_1)}\ldots\lambda_{k\sigma(i_k)} \in \mathbb{F}_q$.

Since ψ is an isomorphism and $\varphi' = \psi^{-1} \circ \varphi$, it follows that φ' is an embedding as well. □

Remark 24 The map φ is called the *Plücker embedding* of the Grassmannian $\mathcal{G}_q(k,n)$. The projective coordinates

$$\begin{aligned}
[\det(U[1,\ldots,k]) : \ldots : \det(U[n-k+1,\ldots,n])] = \mathbb{F}_q^\times(&\det(U[1,\ldots,k]), \ldots, \\
&\det(U[n-k+1,\ldots,n])).
\end{aligned}$$

are often referred to as the *Plücker coordinates* of $\mathrm{rs}(U)$.

Theorem 25 *The following diagram commutes:*

$$\begin{array}{ccc} \mathcal{U} & \xrightarrow{\cdot P} & \mathcal{U}P \\ \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi'} \\ \sum \mu_{i_1,\ldots,i_k}\left(\alpha^{i_1} \wedge \ldots \wedge \alpha^{i_k}\right) * \mathbb{F}_q^\times & \xrightarrow{* \alpha} & \sum \mu_{i_1,\ldots,i_k}\left(\alpha^{i_1+1} \wedge \ldots \wedge \alpha^{i_k+1}\right) * \mathbb{F}_q^\times \end{array}$$

Hence, an irreducible cyclic orbit code $\mathcal{C} = \{\mathcal{U}P^i \mid i = 0, \ldots, \mathrm{ord}(P) - 1\}$ *has a corresponding "Plücker orbit":*

$$\varphi'(\mathcal{C}) = \left\{\varphi'(\mathcal{U}) * \alpha^i \mid i = 0, \ldots, \mathrm{ord}(\alpha) - 1\right\} = \varphi'(\mathcal{U}) * \langle\alpha\rangle$$

Proof

$$\begin{aligned} \varphi'(\mathcal{U}P) &= \mathbb{F}_q^\times \cdot (\phi(U_1P) \wedge \ldots \wedge \phi(U_kP)) = \mathbb{F}_q^\times \cdot (\phi(U_1)\alpha \wedge \ldots \wedge \phi(U_k)\alpha) \\ &= \mathbb{F}_q^\times \cdot (\phi(U_1) \wedge \ldots \wedge \phi(U_k)) * \alpha \end{aligned}$$

□

Example 26 Over $\mathbb{F}_2$ let $p(x) = x^4 + x + 1$ and $\mathcal{U} \in \mathcal{G}_2(2, 4)$ such that $\phi(\mathcal{U}) = \{0, 1, \alpha + \alpha^2, 1 + \alpha + \alpha^2\}$, i.e.

$$\mathcal{U} = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Then $\varphi'(\mathcal{U}) = (1 \wedge \alpha + \alpha^2) = (1 \wedge \alpha) + (1 \wedge \alpha^2)$ and $\varphi(\mathcal{U}) = [\mu_{0,1} : \mu_{0,2} : \mu_{0,3} : \mu_{1,2} : \mu_{1,3} : \mu_{2,3}] = [1 : 1 : 0 : 0 : 0 : 0]$. The elements of the Plücker orbit $\varphi'(\mathcal{U}) * \langle\alpha\rangle$ are

$$\begin{aligned} &(1 \wedge \alpha + \alpha^2) = (1 \wedge \alpha) + (1 \wedge \alpha^2), \\ &(\alpha \wedge \alpha^2 + \alpha^3) = (\alpha \wedge \alpha^2) + (\alpha \wedge \alpha^3), \\ &(\alpha^2 \wedge \alpha^3 + \alpha^4) = (\alpha^2 \wedge 1 + \alpha + \alpha^3) = (\alpha^2 \wedge 1) + (\alpha^2 \wedge \alpha) + (\alpha^2 \wedge \alpha^3), \\ &(\alpha^3 \wedge \alpha + \alpha^2 + \alpha^4) = (\alpha^3 \wedge 1 + \alpha^2) = (\alpha^3 \wedge 1) + (\alpha^3 \wedge \alpha^2), \\ &(\alpha^4 \wedge \alpha + \alpha^3) = (1 + \alpha \wedge \alpha + \alpha^3) = (1 \wedge \alpha) + (1 \wedge \alpha^3) + (\alpha \wedge \alpha^3), \end{aligned}$$

and $(\alpha + \alpha^2 \wedge \alpha^2 + \alpha^4) = (\alpha + \alpha^2 \wedge 1 + \alpha + \alpha^2) = (\alpha + \alpha^2 \wedge 1) = (1 \wedge \alpha + \alpha^2)$ over $\mathbb{F}_2$. The corresponding Plücker coordinates are

$$\begin{aligned} &[1 : 1 : 0 : 0 : 0 : 0], \\ &[0 : 0 : 0 : 1 : 1 : 0], \\ &[0 : 1 : 0 : 1 : 0 : 1], \\ &[0 : 0 : 1 : 0 : 0 : 1], \\ &[1 : 0 : 1 : 0 : 1 : 0]. \end{aligned}$$

The respective subspace code is the spread code defined by $x^4 + x + 1$ according to Sect. 3.1.

In the following we describe the balls of radius t (with respect to the subspace distance) around some $\mathcal{U} \in \mathcal{G}_q(k, n)$ with the help of the Plücker coordinates. An algebraic description of the balls of radius t is potentially important if one is interested in an algebraic decoding algorithm for constant dimension codes. For example, a list decoding algorithm would compute all code words inside some ball around a received message word.

The main result shows that the balls of radius t have the structure of Schubert varieties [5, p. 316]. In order to establish this result we introduce the following partial order:

Definition 27 Consider the set $\binom{[n]}{k} := \{(i_1, \ldots, i_k) \mid i_l \in \mathbb{Z}_n \ \forall l\}$ and define the partial order

$$\mathbf{i} := (i_1, \ldots, i_k) > (j_1, \ldots, j_k) =: \mathbf{j} \iff \exists N \in \mathbb{N}_{\geq 0} : i_l = j_l \ \forall l < N \text{ and } i_N > j_N.$$

It is easy to compute the balls around a vector space in the following special case.

Proposition 28 *Denote the balls of radius* $2t$ *centered at* $\mathcal{U}$ *in* $\mathcal{G}_q(k, n)$ *by* $B_{2t}(\mathcal{U})$ *and define* $\mathcal{U}_0 := \mathrm{rs}[\, I_{k\times k} \ 0_{k\times n-k} \,]$. *Then*

$$\begin{aligned} B_{2t}(\mathcal{U}_0) = \{\mathcal{V} \in \mathcal{G}_q(k, n) \mid \varphi'(\mathcal{V}) = \det(\mathcal{V}[i_1, \ldots, i_k]) = 0 \ \forall (i_1, \ldots, i_k) \\ \not\leq (t+1, \ldots, k, n-t+1, \ldots, n)\} \end{aligned}$$

Proof For $\mathcal{V}$ to be inside the ball it has to hold that

$$\begin{aligned} & d_S(\mathcal{U}_0, \mathcal{V}) \leq 2t \\ \iff \ & 2k - 2\dim(\mathcal{U}_0 \cap \mathcal{V}) \leq 2t \\ \iff \ & \dim(\mathcal{U}_0 \cap \mathcal{V}) \geq k - t, \end{aligned}$$

i.e. $k - t$ many of the unit vectors $e_1, \ldots, e_k$ have to be elements of $\mathcal{V}$. Since $\phi(e_j) = \alpha^{j-1}$, it follows that $\varphi'(\mathcal{V})$ has to fulfill

$$\mu_{i_1,\ldots,i_k} = 0 \text{ if } (i_1, \ldots, i_k) \not\leq (t+1, \ldots, k, n-t+1, \ldots, n).$$

□

The proposition shows that $B_{2t}(\mathcal{U}_0)$ is described in the Plücker space $\mathbb{P}^{\binom{n}{k}-1}$ as a point in the Grassmannian together with linear constraints on the Plücker coordinates.

Example 29 In $\mathcal{G}_2(2, 4)$ we have

$$\mathcal{U}_0 = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

and the elements of distance 2 (i.e. $t = 1$) are

$$\begin{aligned} B_2(\mathcal{U}_0) &= \{\mathcal{V} \in \mathcal{G}_2(2, 4) \mid \det(\mathcal{V}[i_1, i_2]) = 0 \ \forall (i_1, i_2) \not\leq (2, 4)\} \\ &= \{\mathcal{V} \in \mathcal{G}_2(2, 4) \mid \det(\mathcal{V}[3, 4]) = 0\}. \end{aligned}$$

Next we derive the equations for a ball $B_{2t}(\mathcal{U})$ around an arbitrary subspace $\mathcal{U} \in \mathcal{G}_q(k, n)$. For this assume that $\mathcal{U} = \mathcal{U}_0 G$ for some $G \in \mathrm{GL}_n$. A direct computation shows that

$$B_{2t}(\mathcal{U}) = B_{2t}(\mathcal{U}_0 G) = B_{2t}(\mathcal{U}_0)G.$$

The transformation by G transforms the linear equations $\det(\mathcal{V}[i_1, \ldots, i_k]) = 0$ $\forall (i_1, \ldots, i_k) \not\leq (t+1, \ldots, k, n-t+1, \ldots, n)$ into a new set of linear equations in the Plücker coordinates. Instead of deriving these equations in an explicit manner we will show instead that the ball $B_{2t}(\mathcal{U})$ describes a Schubert variety. Then we will show that the equations defining the ball consist of the defining equations of the Grassmann variety together with a set of linear equations describing the Schubert variety.

Definition 30 A flag $\mathcal{F}$ is a sequence of nested subspaces

$$\{0\} \subset V_1 \subset V_2 \subset \ldots \subset V_n = \mathbb{F}_q^n$$

where we assume that $\dim V_i = i$ for $i = 1, \ldots, n$.

Definition 31 Consider the multi-index $\mathbf{i} = (i_1, \ldots, i_k)$ such that $1 \leq i_1 < \ldots < i_k \leq n$. Then

$$S(\mathbf{i}; \mathcal{F}) := \{\mathcal{V} \in \mathcal{G}_q(k, n) \mid \dim(\mathcal{V} \cap V_{i_s}) \geq s\}$$

is called a *Schubert variety*.

One observes that $B_{2t}(\mathcal{U}) = \{\mathcal{V} \in \mathcal{G}_q(k, n) \mid \dim(\mathcal{U} \cap \mathcal{V}) \geq k - t\}$ is nothing else than a special Schubert variety. Indeed, we can simply choose a flag $\mathcal{F}$ having the property that $V_k = \mathcal{U}$ in conjunction with the multi-index $\mathbf{i} = (t + 1, \ldots, k, n - t + 1, \ldots, n)$.

Next we describe the defining equations inside the Plücker space $\mathbb{P}^{\binom{n}{k}-1}$. For this introduce a basis $\{e_1, \ldots, e_n\}$ of $\mathbb{F}_q^n$ which is compatible with the flag $\mathcal{F}$, i.e. $\text{span}\{e_1, \ldots, e_i\} = V_i$ for $i = 1, \ldots, n$.

The basis $\{e_1, \ldots, e_n\}$ induces the basis

$$\{e_{i_1} \wedge \ldots \wedge e_{i_k} \mid 1 \leq i_1 < \cdots < i_k \leq n\}$$

of $\Lambda^k(\mathbb{F}_q^n)$. If $x \in \Lambda^k(\mathbb{F}_q^n)$, denote by $x_{\mathbf{i}}$ its coordinate with regard to the basis vector $e_{i_1} \wedge \ldots \wedge e_{i_k}$. The defining equations of the Schubert variety $S(\mathbf{i}; \mathcal{F})$ are then given by

$$S(\mathbf{i}; \mathcal{F}) = \{x \in \mathcal{G}_q(k, n) \mid x_{\mathbf{j}} = 0, \ \ \forall \mathbf{j} \not\leq \mathbf{i}\}.$$

An elementary proof of the fact that these linear equations together with the defining equations of the Grassmannian $\mathcal{G}_q(k, n)$ indeed describe the Schubert variety $S(\mathbf{i}; \mathcal{F})$ can be found in [5, Chap. XIV].

For coding theory it is important to note that we have explicit equations describing Schubert varieties in general and balls of radius t in particular. If a constant dimension network code is given by explicit equations, one would immediately have a description of all code words which are closer than a given distance to some received subspace.

5 Conclusion

We listed all possible irreducible cyclic orbit codes and showed that it suffices to investigate the groups generated by companion matrices of irreducible polynomials. Moreover, polynomials of the same degree and same order generate codes with the same cardinality and minimum distance. These two properties of the code depend strongly on the choice of the starting point in the Grassmannian. We showed how one can deduce the size and distance of an orbit code for a given subgroup of GL_n from the starting point $\mathcal{U} \in \mathcal{G}_q(k, n)$. For primitive groups this is quite straight-forward while the non-primitive case is more difficult.

Subsequently one can use this theory of irreducible cyclic orbit codes to characterize all cyclic orbit codes.

Finally we described the irreducible cyclic orbit codes within the Plücker space and showed that the orbit structure is preserved. Moreover, we showed how balls around an element of the Grassmann variety can be described using Plücker coordinates.

Acknowledgments Research partially supported by Swiss National Science Foundation Project no. 126948. A preliminary version of this paper was presented at the Seventh International Workshop on Coding and Cryptography (WCC) 2011.

References

1. Ahlswede R., Cai N., Li S.-Y.R., Yeung R.W.: Network information flow. IEEE Trans. Inf. Theor. **46**, 1204–1216 (2000).
2. Elsenhans A., Kohnert A., Wassermann A.: Construction of codes for network coding. In: Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems—MTNS, pp. 1811–1814. Budapest (2010).
3. Etzion T., Silberstein N.: Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. IEEE Trans. Inf. Theor. **55**(7), 2909–2919 (2009).
4. Hirschfeld J.W.P.: Projective Geometries Over Finite Fields. Oxford Mathematical Monographs 2nd edn. The Clarendon Press Oxford University Press, New York (1998).
5. Hodge W.V.D., Pedoe D.: Methods of Algebraic Geometry, Vol. II. Cambridge University Press (1952).
6. Kohnert A., Kurz S.: Construction of large constant dimension codes with a prescribed minimum distance. In: Jacques C., Willi G., Müller-Quade Jörn (eds.), MMICS, vol. 5393 of Lecture Notes in Computer Science. Springer, pp. 31–42 (2008).
7. Kötter R., Kschischang F.R.: Coding for errors and erasures in random network coding. IEEE Trans. Inf. Theor. **54**(8), 3579–3591 (2008).
8. Lidl R., Niederreiter H.: Introduction to Finite Fields and their Applications. Cambridge University Press, Cambridge, London (1986).
9. Manganiello F., Gorla E., Rosenthal J.: Spread codes and spread decoding in network coding. In: Proceedings of the 2008 IEEE International Symposium on Information Theory, pp. 851–855. Toronto, Canada (2008).
10. Manganiello F., Trautmann A.-L., Rosenthal J.: On conjugacy classes of subgroups of the general linear group and cyclic orbit codes. In: Proceedings of the 2011 IEEE International Symposium on Information Theory, pp. 1916–1920, 31, 5 Aug (2011).
11. Manganiello F., Trautmann A.-L.: Spread decoding in extension fields. arXiv:1108.5881v1 [cs.IT], (2011).
12. Silva D., Kschischang F.R., Kötter R.: A rank-metric approach to error control in random network coding. Proc. IEEE Int. Symp. Inf. Theor. **54**(9), 3951–3967 (2008).
13. Trautmann A.-L., Manganiello F., Rosenthal J.: Orbit codes—a new concept in the area of network coding. In: Information Theory Workshop (ITW), IEEE, pp. 1–4, Dublin August (2010).